UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,446	12/26/2000	Guenter Karjoth	SZ999-012	4185

7590 07/30/2004

Ronald L. Drumheller, Esq
94 Teakettle Spout Road
Mahopac, NY 10541

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/748,446	KARJOTH ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-10 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-10 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 26 December 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 have been examined.

Priority

2. Receipt is acknowledged of papers filed under 35 U.S.C. 119 (a)-(d) based on an application filed in Europe (EPO) on 12/24/1999. Applicant has not complied with the requirements of 37 CFR 1.63(c), since the oath, declaration or application data sheet does not acknowledge the filing of any foreign application. A new oath, declaration or application data sheet is required in the body of which the present application should be identified by application number and filing date.

Specification

3. The abstract of the disclosure is objected to because of the words "taylored" (line 13) and "minimes" (line 15). Correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-7 and 9-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claims 1 and 9-10, a broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claims 1 and 9-10 recite the broad recitation “a device” (see preamble), and the claim also recites “a portable device with limited processing power and/or memory” (see preamble) which is the narrower statement of the range/limitation.

b. Claims 2-7 are rejected on the same basis as claim 1 recited in paragraph 5a by virtue of their dependencies.

c. Regarding claims 1 and 9-10, the phrase "in particular" in the preamble renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

d. Claims 2-7 are rejected on the same basis as claim 1 recited in paragraph 5c by virtue of their dependencies.

e. Regarding claim 1, it recites the limitation "until a previously verified authentication value << has this value a name??>> is reached". The notation << has this value a name??>> is not appropriate for claim language. In addition, it has not been discussed in the specification. Therefore, it's not clear what the limitation is. For examination purposes, the limitation is interpreted as "until a previously verified authentication value is reached" (see specification, page 22, lines 16-18).

f. Claims 2-7 are rejected on the same basis as claim 1 recited in paragraph 5e by virtue of their dependencies.

g. Regarding claim 3, a broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claims 1 and 9-10 recite the broad recitation "a hash tree" (3rd line), and the claim also recites "a binary and/or symmetrical tree" (3rd line) which is the narrower statement of the range/limitation.

h. Regarding claim 3, the phrase "in particular" (3rd line) renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

6. Claims 1-7 are is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements. See MPEP § 2172.01.

Regarding claim 1, the omitted elements are: selected branch authentication values are not included in messages ***Mi*** (claim 1, the step of generating messages ***Mi***). Referring to page 21, lines 4-24 and figure 1 in the specification, it would not be able to authenticate blocks ***B1*** and ***B5*** according to the claimed method if the branch authentication values ***H2***, ***H6*** and ***H4*** were included in the corresponding messages ***M1*** and ***M5***.

Claims 2-7 are rejected on the same basis as claim 1 by virtue of their dependencies.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-4, 6 and 8-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Wong et al. ("Digital Signatures for Flows and Multicasts").

a. Regarding claim 1, which is representative of claims 8-10, Wong discloses a method for downloading data from a provider (AP) via a transmission channel of limited bandwidth onto a device (SC) (Section I-B, page 503, "We have observed various ... mobile computers using wireless communication.") characterized by

at the provider (AP), generating packets ***Bi***, which meet the limitation of code blocks, of the data to be transmitted (Section II-B, page 504, "Tree chaining subsumes star ... eight packets with packet digests"),

defining an authentication function comprising a one-way function (Section II-A, page 504, "Consider m packets that ... with some digital signature scheme"),

computing an authentication value ***H(Bi)*** for each block ***Bi*** to be transmitted (Section II-B, page 504, "Tree chaining subsumes star ... eight packets with packet digests"),

selecting an authentication tree for said authentication values ***H(Bi)*** (Section II-B, page 504-505 and figure 2),

computing authentication values ***Hi*** of the branches and the root authentication value ***HT*** of said tree (Section II-B, page 504-505 and figure 2),

signing said root authentication value ***HT*** thereby generating ***Sign(HT)*** (Section II-A, page 504, "Consider m packets that ... with some digital signature scheme"),

generating messages ***Mi*** comprising said blocks ***Bi*** and, partly, selected ones of said authentication values ***H(Bi)*** and ***Hi*** (Section II-B, page 505, "For a packet to be individually ... in the packet's path to the root"),

transmitting said signed root authentication value ***Sign(HT)*** and said messages ***Mi*** from said provider (AP) to said device (SC) (Section II-B, page 505, "For a packet to be individually ... in the packet's path to the root"),

in said device (SC), upon receiving any one of said messages ***Mi***, extracting said block ***Bi***, computing the corresponding authentication value ***H(Bi)*** and cashing it, computing selected intermediate authentication values ***Hi*** along said tree until a previously verified authentication value is reached (Section II-B, page 505, "To verify a packet ... the sixth packet is verified"),

comparing said computed intermediate authentication value ***Hi*** with said previously verified authentication value and (Section II-B, page 505, "To verify a packet ... the sixth packet is verified"),

if the values are equal, accepting said received block ***Bi*** or, if otherwise, indicating an error (Section II-B, page 505, "To verify a packet ... the sixth packet is verified").

b. Regarding claim 2, Wong further discloses that the generated code blocks ***Bi*** of the data to be transmitted are sequentially transmitted (Section I-A, page 502, "A flow is a sequence ... generated by the same source"), the computing and comparing in the device (SC) is executed in any order including sequentially until all blocks ***Bi*** that are

received are verified, and the data is considered correctly received, when no error was indicated (Section II-B, page 504-505).

c. Regarding claim 3, Wong further discloses that the one-way function of the authentication function is a hashing function (Section II-A, page 504, "Consider m packets that ... with some digital signature scheme") and the authentication tree is a binary and symmetrical tree, of the code blocks ***Bi*** generated in the provider (AP) (fig. 2).

d. Regarding claim 4, Wong further discloses that a process is defined in the provider (AP), consisting of a several loops which iteratively construct an ***i***-th message ***Mi*** consisting a block Bi plus one or more authentication values ***Hi*** and/or ***H(Bi)*** (Section II-B, page 505, "For a packet to be individually ... in the packet's path to the root").

e. Regarding claim 6, Wong further discloses that a process is defined in the device (SC), consisting of several loops, said process iteratively evaluating an ***i***-th message ***Mi*** by extracting from a received messages ***Mi*** the corresponding block ***Bi*** and, if the received message ***Mi*** includes one or more authentication values ***Hi*** and/or ***H(Bi)***, extracting these values and caching them for later verification (Section II-B, page 505, "Suppose the third packet ... the authentication tree at most once").

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong as applied to claim 4 above, and further in view of Merkle (4,309,569). Wong discloses that each message ***Mi*** for a corresponding block ***Bi*** includes the siblings of each node in the block' path to the root, which is equivalent to a full authentication path from the corresponding block ***Bi*** towards the root of the authentication tree (Section II-B, page 505, "For a packet to be individually ... in the packet's path to the root"). Wong does not teach that each 2j-th message ***Mi*** consists of the corresponding block ***Bi*** alone. However, Wong discloses that blocks ***B1*** and ***B2*** share the same parent (Section II-B, page 505, "For example, the parent of ... being the signed block digest") in an authentication tree. One of ordinary skill in the art would recognize that the blocks ***B1*** and ***B2*** share the same authentication path from their parent towards the root of the authentication tree. Since the same authentication path from the parent towards the root is sent twice, first with block ***B1*** in message ***M1*** and then with block ***B2*** in message ***M2***, the information is redundant. Merkle discloses an authentication method using a binary authentication tree similar to that of Wong. Merkle teaches not transmitting redundant authentication information in order to reduce the transmission load (fig. 1; col. 3, lines 3-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the Wong method such that the authentication path from the parent of block ***B2*** is considered redundant and not transmitted, as taught by Merkle; accordingly, the message ***M2***, and all even-indexed messages in general,

consists of the corresponding block ***Bi*** alone. The motivation for doing so would have been to reduce transmission load.

11. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong as applied to claim 6 above, and further in view of Gennaro et al. ("How to Sign Digital Streams"). Wong discloses storing in the device (SC) authentication values ***H(Bi)*** and/or ***Hi*** and/or ***HT*** needed to authenticate subsequently transmitted block ***Bi*** (Section II-B, page 505, "Suppose the third packet ... the authentication tree at most once"). Wong does not disclose clearing all authentication values not needed in further process. Gennaro discloses clearing all authentication values not needed in further process (Section 3, page 188, "Thus the receiver has to ... no big table is needed in memory"). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the Wong method such that all authentication values not needed in further process are cleared, as taught by Gennaro, so that no big table is needed in memory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD
Minh Dinh
Examiner
Art Unit 2132

MD
7/20/04

JUSTIN T. DARROW
PRIMARY EXAMINER